IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	:	10/783,558	Confirmation No. 7539
Appellants	:	Robert F. Day, *et al.*	
Filed	:	February 20, 2004	
Group Art Unit:		2439	
Examiner	:	Roderick Tolentino	
Title	:	METHOD AND SYSTEM FOR PROTECTING USER CHOICES	
Docket No.	:	304666.01/MFCP.143750	
Customer No.	:	45809	

VIA EFS – December 13, 2011
Mail Stop Appeal Brief-Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

APPELLANTS' APPEAL BRIEF

Dear Sir:

This is an Appeal from a Final Office Action mailed 10 March 2011, rejecting claims 1-13, 15-25, and 27-29. These claims have been at least twice rejected. Appellants, having filed a Notice of Appeal within the time period provided under 37 C.F.R. § 41.31(a) accompanied by the fee set forth in 37 C.F.R. § 41.20(b)(1), do hereby submit this Appeal Brief along with the fee set forth in 37 C.F.R. § 41.20(b)(2). The Commissioner is hereby authorized to charge any additional fee that may be due, or credit any overpayment, to Deposit Account No. 19-2112 referencing Attorney Docket Number 304666.01/MFCP.143750.

Contents

I. REAL PARTY IN INTEREST

The real party in interest is Microsoft Corporation, a corporation of the State of Washington, United States of America.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF CLAIMS

Claims 1-13, 15-25, and 27-29 are rejected and pending, and the rejection of each of those claims is being appealed. Claims 14 and 26 are canceled.

IV. STATUS OF AMENDMENTS

An amendment was filed on 28 December 2010, before the Final Office Action dated 10 March 2010. That amendment was entered. No amendments were made to the claims after the Final Office Action. A listing of all claims currently pending is reproduced in the Claims Appendix.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The instant application includes three independent claims: claims 1, 12, and 19.

Claim 1

Claim 1 defines a method (**102**) for prioritizing user application preferences based on user input data. In accordance with the method, a computing device is provided. *Appellants' specification, at p. 5, ll. 12-28.* The computing device (**200**) recognizes user input data relevant to a first application as a prioritized user choice setting associated with the first application. The prioritized user choice setting determines at least one property of execution of at least one event of the first application. *Appellants' specification, at p. 7, ll. 5-15.* The user choice setting is secured at the computing device (**200**) as a protected value using an access control indicator. *Appellants' specification, at p. 7, ll. 15-18.* The access control indicator prohibits a second application from modifying the prioritized user choice setting associated with the first application without authorization from the user. *Appellants' specification, at p. 12, ll. 3-11.* The computing device (**200**) receives a request from the second application to modify the prioritized user choice setting associated with the first application. *Appellants' specification, at p. 12, ll. 12-15.* In response to receiving the request from the second application, an approval user interface is generated on the computing device (**200**). *Appellants' specification, at p. 12, ll. 15-20.* The approval user interface requests authorization from the user to modify the prioritized user choice setting associated with the first application to be consistent with the modification request received from the second application. *Appellants' specification, at p. 12, ll. 15-20.* The computing device (**200**) receives input from the user approving the modification of the prioritized user choice setting associated with the first application to be consistent with the modification request received from the second application.

Appellants' specification, at p. 12, ll. 20-25. In turn, the computing device (**200**) modifies the access control indicator to permit modification of the prioritized user choice setting associated with the first application to be consistent with the modification request received from the second application. *Appellants' specification, at p. 12, ll. 25-30.* The prioritized user choice setting is modified to a different value in accordance with the received user input at the computing device (**200**). *Appellants' specification, at p. 13, ll. 10-16.* The computing device (**200**) restores the access control indicator to prohibit further modification by the second application of the prioritized user choice setting associated with the first application. *Appellants' specification, at p. 13, ll. 17-21.*

Claim 12

Claim 12 defines a system for storing user choice settings in a data repository to prevent undesired modifications to user choice settings. The system comprises a registry (**106**), access control list (**112**), and an approval user interface (**116**). *Appellants' specification, at p. 8.* The registry (**106**), stores a user choice setting associated with a first application as a protected value in a registry key. *Id.* The user choice setting determines at least one property of execution of at least one event of the first application. *Appellants' specification, at p. 7, l. 5.* The user choice setting comprises at least one of a user preference relating to a file association, an autoplay setting, contents of a start menu, a registered client, a protocol handler, a MIME type handler, a task association, an internet explorer home page, a reset Web page setting, and a sidebar setting. *Id.* The access control list (ACL) (**112**) secures the registry key. *Appellants' specification, at p. 8, ll. 5-16.* The ACL (**112**) prevents the first application or another application from modifying the user choice setting associated with the first application. *Appellants' specification, at p. 8, ll. 16-25.* The approval user interface (**116**) controls

modifications to the user choice setting. *Id.* The approval user interface (**116**) is generated on a computing device (**200**) of the user in response to receiving a request from the first application or another application to modify the user choice setting. *Appellants' specification, at p. 10, ll. 17-25.* The approval user interface (**116**), upon obtaining approval to modify the user choice setting, modifies the ACL (**112**) to permit writing to change the protected value in the registry key to a modified user choice setting. *Appellants' specification, at p. 10, ll. 25-30.*

Claim 19

Claim 19 defines computer-accessible storage media having machine executable instructions components for performing a method of safely modifying user application preferences for when and how an application is to operate on a computer (**200**) of a user. *Appellants' specification, at p. 8, ll. 16-25.* In accordance with the method, user input data relevant to the application is recognized as a prioritized user choice setting. The prioritized user choice setting determines at least one property of execution of at least one event of the application. *Appellants' specification, at p. 7, ll. 1-17.* The prioritized user choice setting is secured as a protected value using an access control indicator. *Id.* The access control indicator prohibits the application from modifying the prioritized user choice setting. *Appellants' specification, at p. 8, ll. 5-15.* A request from the application to modify the prioritized user choice setting is received. *Appellants' specification, at p. 10, ll. 16-25.* In response to the request from the application to modify the prioritized user choice setting, an approval user interface (**116**) requesting authorization from the user is generated to modify the prioritized user choice setting in accordance with the modification request received. *Id.* Input is received from the user approving modification of the prioritized user choice setting associated with the application to be consistent with a value stated in the request received from the application. *Appellants' specification, at p. 12, ll. 20-27.* The access control indicator is modified to permit

modification of the prioritized user choice setting associated with the application to match the value stated in the request received from the application. *Appellants' specification, at p. 13, ll. 1-16.* In turn, the prioritized user choice setting is modified to match the value stated in the request received from the application in accordance with the received user input. *Id.* The access control indicator is restored to prohibit further modification of the prioritized user choice setting. *Appellants' specification, at p. 13, ll. 16-25.* A change notification to the user is generated once the prioritized user choice setting has been modified. *Appellants' specification, at p. 11, ll. 10-15.*

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A) Whether claims 1, 12 and 19 are obvious under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Publication No. 2004/0199763 ("Freund"), U.S. Patent Publication No. 2004/0003279 ("Beilinson"), and U.S. Patent Publication No. 2004/0193606 ("Arai").

B) Whether claims 2-8, 10-11, 15-18, 20-25, and 28-29 are obvious under 35 U.S.C. § 103(a) as being unpatentable over Freund, Beilinson, Arai, and U.S. Patent Publication No. 2002/0143961 ("Siegel").

C) Whether claims 9, 13, and 27 are obvious under 35 U.S.C. § 103(a) as being unpatentable over Freund, Beilinson, Arai, Siegel, and U.S. Patent No. 6,370,141 ("Giordano III").

D) Whether claim 19 and its dependent claims are non-statutory subject matter under 35 U.S.C. § 101.

VII. ARGUMENT

Title 35 U.S.C. § 103(a) declares a patent shall not issue when "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." The Supreme Court in *Graham v. John Deere* counseled that an obviousness determination is made by identifying: the scope and content of the prior art; the level of ordinary skill in the prior art; the differences between the claimed invention and prior art references; and secondary considerations[1]. *Graham v. John Deere Co.*, 383 U.S. 1 (1966). The Supreme Court explained, "it will be necessary for [the Office] to look at interrelated teachings of multiple [prior art references]; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by [one of] ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the [patent application]." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007). The apparent reason must be explicitly articulated. *Id.*

A) U.S. Patent Publication No. 2004/0199763 ("Freund"), U.S. Patent Publication No. 2004/0003279 ("Beilinson"), and U.S. Patent Publication No. 2004/0193606 ("Arai") fail to render the invention of independent claims 1, 12 and 19 obvious under 35 U.S.C. § 103(a) because Freund, Beilinson, and Arai fail to describe or suggest, among other things, generating an approval user interface on the computing device of the user, the approval user interface requesting authorization from the user to modify the prioritized

[1] Appellants respectfully remind the Office that "Office personnel fulfill the critical role of factfinder . . . Office personnel must therefore ensure that the written record includes findings of fact concerning the state of the art and the teachings of the references applied. In certain circumstances, it may also be important to include explicit findings as to how a person of ordinary skill would have understood prior art teachings. See, MPEP § 2141. The Office has failed to establish that Freund, Beilinson, and Arai fairly describes or suggests all elements of claims 1, 12 and 19. For instance, the record is devoid of any findings regarding the scope and content (e.g., shortcomings) of the references and the differences between the invention of claims 1, 12, and 19 and the references. Further, there are no findings regarding the registry, registry values, registry key, and ACL of dependent claims 2, 9-11, 20, 27-29 and independent claim 12. Furthermore, as explained in detail below, Siegel and Giordano do not remedy the deficiencies of Freund, Beilinson, and Arai with respect to the elements of the independent claims 1, 12, and 19 and dependent claims 2, 9-11, 20, and 27-29. Thus, Appellants take the Office's silence with regard to shortcomings of the references and the combination of multiple references as an admission that Freund, Beilinson, Arai, Siegel, and Giordano alone and in combination cannot render the invention of the claims unpatentable.

user choice setting associated with the first application to be consistent with the modification request received from the second application.

(i) Claim 1

It is respectfully submitted that the cited art, including Freund, Beilinson, and Arai, fails to describe or suggest, among other things, *securing, at the computing device of the user, the user choice setting as a protected value using an access control indicator, wherein the access control indicator prohibits a second application from modifying the prioritized user choice setting associated with the first application without authorization from the user; receiving, at the computing device of the user, a request from the second application to modify the prioritized user choice setting associated with the first application; in response to receiving the request from the second application to modify the prioritized user choice setting associated with the first application, generating an approval user interface on the computing device of the user, the approval user interface requesting authorization from the user to modify the prioritized user choice setting associated with the first application to be consistent with the modification request received from the second application,* as recited in independent claim 1.

The Office relies upon Freund, at paragraph [0023]; Beilinson, at paragraphs [0006] and [0065]; and Arai, at paragraphs [0002] and [0013] to render the invention of independent claim 1 unpatentable.

a. Freund in combination with Beilinson and Arai fail to describes or suggest securing the user choice setting

The Office admits that Beilinson and Arai alone and in combination do not describe or suggest securing, at the computing device of the user, the user choice setting as a protected value using an access control indicator, wherein the access control indicator prohibits a second application from modifying the prioritized user choice setting associated with the first

application without authorization from the user. The Office alleges that Freund, at paragraph [0023], in combination with Beilinson and Arai describes or suggest this element.

Freund, at paragraph [0023], in combination with Beilinson and Arai do not describe or suggest securing, at the computing device of the user, the user choice setting as a protected value using an access control indicator, wherein the access control indicator prohibits a second application from modifying the prioritized user choice setting associated with the first application without authorization from the user as recited in claim 1.

In fact, the cited portions of Freund describe a method of blocking attempts to invoke a system service based on rules that specify the services accessible by an application. Freund, at paragraph [0023], explains that communications between processes are monitored and allowed based on policy rules. At best, Freund, at paragraphs [0023], [0041-0043] and [0079]-[0082], prevents an application from accessing a communication service, e.g., Internet service. Freund fails to describe or suggest securing, at the computing device of the user, the user choice setting as a protected value using an access control indicator. Freund fails to describe or suggest an access control indicator that prohibits a second application from modifying the prioritized user choice setting associated with the first application without authorization from the user. Beilinson and Arai in combination with Freund do not describe or suggest the access control indicator that prohibits modification of a user choice setting. Nothing in Beilinson and Arai in combination with Freund describes or suggests a second application that is prohibited from modifying the prioritized user choice setting associated with the first application without authorization from the user. Furthermore, Beilinson and Arai in combination with Freund fails to describe or suggest a user choice setting that is a protected value as recited in independent claim 1.

b. Beilinson, in combination with Freund and Arai fail to describe or suggest receiving a request from the second application to modify the prioritized user choice setting associated with the first application.

The Office admits that Freund and Arai alone and in combination do not describe or suggest receiving, at the computing device of the user, a request from the second application to modify the prioritized user choice setting associated with the first application. The Office alleges that Beilinson, at paragraph [0065], in combination with Freund and Arai describes or suggests this element.

Beilinson, at paragraph [0065], in combination with Freund and Arai fails to describe or suggest receiving, at the computing device of the user, a request from the second application to modify the prioritized user choice setting associated with the first application.

Beilinson, at paragraphs [0006] and [0065], describes an administrator that restricts a user's logon hours, logon duration, access to computer functions, and access to applications based on content rating. For instance, Beilinson is directed to parental control of a minor's computer activity. At best, Beilinson, at paragraphs [0065]-[0071], explains that a user may request temporary increases in access privileges set by an administrator that limits access by the user via a group policy engine. Beilinson does not describe or suggest that the user request is made via a second application. Beilinson does not describe or suggest that the second application requests modification of user choice settings associated with a first application. Beilinson does not describe or suggest that the modification is of user choice settings associated with a first application are for at least one execution property of an event associated with the first application as opposed to administrator settings that limit access by the user.

Nothing in Beilinson in combination with Freund and Arai describes or suggests receiving, at the computing device of the user, a request from the second application to modify

the secured prioritized user choice setting associated with the first application. Beilinson in combination with Freund and Arai does not describe or suggest a second application that modifies settings associated with a first application. Furthermore, Beilinson in combination with Freund and Arai fails to describe or suggest user choice setting of a first application, where a second application requests modification of the user choice settings.

c. <u>Beilinson in combination with Freund and Arai fail to describe or suggest in response to receiving the request from the second application to modify the prioritized user choice setting associated with the first application, generating an approval user interface on the computing device of the user, the approval user interface requesting authorization from the user to modify the prioritized user choice setting associated with the first application to be consistent with the modification request received from the second application.</u>

The Office admits that Freund and Arai alone and in combination do not describe or suggest in response to receiving the request from the second application to modify the prioritized user choice setting associated with the first application, generating an approval user interface on the computing device of the user, the approval user interface requesting authorization from the user to modify the prioritized user choice setting associated with the first application to be consistent with the modification request received from the second application. The Office alleges that Beilinson, at paragraph [0065], in combination with Freund and Arai describes or suggests this element.

Beilinson, at paragraph [0065], in combination with Freund and Arai fails to describe or suggests in response to receiving the request from the second application to modify the prioritized user choice setting associated with the first application, generating an approval user interface on the computing device of the user, the approval user interface requesting authorization from the user to modify the prioritized user choice setting associated with the

first application to be consistent with the modification request received from the second application.

As discussed above, paragraphs [0065]-[0071] of Beilinson explain that a user may request temporary increases in access privileges set by an administrator that limit access by the user. In turn, the administrator receives the request and denies or authorizes the request received from the user. Beilinson fails to describe or suggest authorizing a change in a secured user setting by the user as opposed to the administrator. Beilinson fails to describe or suggest changing the user setting associated with a first application based on the request received from a second application that is different from the first application. Beilinson fails to describe or suggest a computing device that generates an approval interface for the user that established the secured user choice settings with a first application. Beilinson fails to describe or suggest authorizing modification based on the changes received from the request of a second application. Nothing in Beilinson in combination with Freund and Arai[2] describes or suggests generating an approval user interface on the computing device of the user, the approval user interface requesting authorization from the user to modify the prioritized user choice setting associated with the first application to be consistent with the modification request received from the second application.

[2] Arai, at paragraphs [0002] and [0013], describes a system for managing system policies. Arai describes an interface that is used to establish a policy. However, nothing in Arai in combination with Freund and Beilinson describe or suggest securing, at the computing device of the user, the user choice setting as a protected value using an access control indicator, wherein the access control indicator prohibits a second application from modifying the prioritized user choice setting associated with the first application without authorization from the user. Arai in combination with Freund and Beilinson does not describe or suggest the access control indicator that prohibits modification of a user choice setting. Furthermore, Arai in combination with Freund and Beilinson fails to describe or suggest a user choice setting that is a protected value or the approval interface as recited in independent claim 1. For at least the above reasons, Beilinson and Arai fail to remedy the deficiencies of Freund with respect to all elements of independent claim 1. Accordingly, the combination of Freund, Beilinson, and Arai fails to teach or suggest all elements of independent claim 1

(ii) Claim 12

It is respectfully submitted that the cited art, including Freund, Beilinson, and Arai, fails to describe or suggest, among other things, *a registry for storing a user choice setting associated with a first application as a protected value in a registry key, wherein the user choice setting determines at least one property of execution of at least one event of the first application, and wherein the user choice setting comprises at least one of a user preference relating to a file association, an autoplay setting, contents of a start menu, a registered client, a protocol handler, a MIME type handler, a task association, an internet explorer home page, a reset Web page setting, and a sidebar setting; and an access control list (ACL) to secure the registry key, wherein the ACL prevents the first application or another application from modifying the user choice setting associated with the first application;* as recited in independent claim 12.

The Office relies upon Freund, at paragraph [0023]; Beilinson, at paragraphs [0006] and [0065]; and Arai, at paragraphs [0002] and [0013] to render the invention of independent claim 12 unpatentable.

a. A *prima facie* case of obviousness cannot be established because the record in incomplete

The Office, however, makes no factual finding for a registry for storing a user choice setting associated with a first application as a protected value in a registry key, wherein the user choice setting determines at least one property of execution of at least one event of the first application, and wherein the user choice setting comprises at least one of a user preference relating to a file association, an autoplay setting, contents of a start menu, a registered client, a protocol handler, a MIME type handler, a task association, an internet explorer home page, a reset Web page setting, and a sidebar setting.

The Office, also, makes no factual finding for an access control list (ACL) to secure the registry key, wherein the ACL prevents the first application or another application from modifying the user choice setting associated with the first application.

Because these non-existent factual findings are not explicitly included in the record, Appellants respectfully submit that a *prima facie* case of obviousness is not established for independent claims 12 and dependent claims 13 and 15-18. Accordingly, Appellants request withdrawal of the obviousness rejection and allowance of independent claim 12 and dependent claims 13 and 15-18.

b. Freund in combination with Beilinson and Arai fail to describe or suggest a registry for storing a user choice setting associated with a first application as a protected value in a registry key

Appellants, based on the sparse record provided by the Office, surmise that the Office admits Beilinson and Arai alone and in combination do not describe or suggest a registry for storing a user choice setting associated with a first application as a protected value in a registry key, wherein the user choice setting determines at least one property of execution of at least one event of the first application, and wherein the user choice setting comprises at least one of a user preference relating to a file association, an autoplay setting, contents of a start menu, a registered client, a protocol handler, a MIME type handler, a task association, an internet explorer home page, a reset Web page setting, and a sidebar setting. The Office appears to allege Freund, at paragraph [0023], in combination with Beilinson and Arai describes or suggests this element.

As discussed above, the cited portions of Freund describe a method of blocking attempts to invoke a system service based on rules that specify the services accessible by an application. Freund, however, does not describe or suggest a registry for storing a user choice

setting associated with a first application as a protected value in a registry key as recited in independent claim 12. Freund fails to describe or suggest the user choice setting determines at least one property of execution of at least one event of the first application. Freund fails to describe or suggest the user choice setting comprises a user preference relating to a file association. Freund fails to describe or suggest the user choice setting comprises an autoplay setting. Freund fails to describe or suggest the user choice setting comprises contents of a start menu. Freund fails to describe or suggest the user choice setting comprises a registered client. Freund fails to describe or suggest the user choice setting comprises a protocol handler. Freund fails to describe or suggest the user choice setting comprises a MIME type handler. Freund fails to describe or suggest the user choice setting comprises a task association. Freund fails to describe or suggest the user choice setting comprises an internet explorer home page. Freund fails to describe or suggest the user choice setting comprises a reset Web page setting. Freund fails to describe or suggest the user choice setting comprises a sidebar setting. Freund in combination with Beilinson and Arai does not fairly describe or suggest a registry for storing a user choice setting associated with a first application as a protected value in a registry key, wherein the user choice setting determines at least one property of execution of at least one event of the first application, and wherein the user choice setting comprises at least one of a user preference relating to a file association, an autoplay setting, contents of a start menu, a registered client, a protocol handler, a MIME type handler, a task association, an internet explorer home page, a reset Web page setting, and a sidebar setting.

c. Freund in combination with Beilinson and Arai fail to describe or suggest an access control list (ACL) to secure the registry key, wherein the ACL prevents the first application or another application from modifying the user choice setting associated with the first application

Appellants again surmise that the Office admits Beilinson and Arai alone and in combination do not describe or suggest an access control list (ACL) to secure the registry key, wherein the ACL prevents the first application or another application from modifying the user choice setting associated with the first application. The Office appears to allege Freund, at paragraph [0023], in combination with Beilinson and Arai describes or suggests this element.

Freund, in combination with Beilinson and Arai, fails to describe or suggests an access control list (ACL) to secure the registry key, wherein the ACL prevents the first application or another application from modifying the user choice setting associated with the first application. As previously mentioned Freund prevents access to a particular service. However, Freund fails to describe or suggest an access control list that secures a registry key value associated with user choice setting of the first application. Freund also fails to describe or suggest an ACL that prevents the first application or another application from modifying the user choice setting that is stored in the registry key. Freund in combination with Beilinson and Arai[3] does not fairly describe or suggest an access control list (ACL) to secure the registry key, wherein the ACL prevents the first application or another application from modifying the user choice setting associated with the first application.

---

[3] Beilinson and Arai fail to remedy the deficiencies of Freund with respect to all elements of independent claim 12. Accordingly, the combination of Freund, Beilinson, and Arai fails to teach or suggest all elements of independent claim 12. Beilinson merely describes an administrator that restricts a user's logon hours, logon duration, access to computer functions, and access to applications based on content rating. Beilinson does not describe or suggest the registry and access control elements of specific registry values as recited in independent claim 12. Arai describes a system for managing system policies. Arai describes an interface that is used to establish a policy. However, nothing in Arai describes or suggests user choice setting that are protected values in a registry having an access control list. The access control list prohibits the first application that is associated with the user choice setting or another application that is not associated with the user choice setting from modifying the protected user choice setting. The protected user choice setting associated with the first application is not modified without authorization from the user. Arai does not describe or suggest an access control list (ACL) to secure the registry key, where the ACL prevents the first application or another application from modifying the user choice setting associated with the first application as recited in independent claim 12.

(iii) Claim 19

It is respectfully submitted that the cited art, including Freund, Beilinson, and Arai, fails to describe or suggest, among other things, *securing the prioritized user choice setting as a protected value using an access control indicator, wherein the access control indicator prohibits the application from modifying the prioritized user choice setting; receiving a request from the application to modify the prioritized user choice setting; and in response to the request from the application to modify the prioritized user choice setting, generating an approval user interface requesting authorization from the user to modify the prioritized user choice setting in accordance with the modification request received,* as recited in independent claim 19.

The Office relies upon Freund, at paragraph [0023]; Beilinson, at paragraphs [0006] and [0065]; and Arai, at paragraphs [0002] and [0013] to render the invention of independent claim 19 unpatentable.

a. Freund in combination with Beilinson and Arai fail to describe or suggest securing the prioritized user choice setting as a protected value using an access control indicator

Appellants, based on the sparse record provided by the Office, surmise that the Office admits Beilinson and Arai alone and in combination do not describe or suggest securing the prioritized user choice setting as a protected value using an access control indicator, wherein the access control indicator prohibits the application from modifying the prioritized user choice setting. The Office appears to allege Freund, at paragraph [0023], in combination with Beilinson and Arai describes or suggests this element.

As discussed above, the cited portions of Freund describes a method of blocking attempts to invoke a system service based on rules that specify the services accessible by an

application. Freund, however, does not describe or suggest securing the prioritized user choice setting. Freund does not describe or suggest a user choice setting is a protected value. Freund fails to describe or suggest an access control indicator that prohibits the application—the same application that established the value for the prioritized user choice setting—from modifying the prioritized user choice setting as recited in independent claim 19. Freund, Beilinson, and Arai, alone and in combination, fail to describe or suggest securing the prioritized user choice setting as a protected value using an access control indicator, wherein the access control indicator prohibits the application from modifying the prioritized user choice setting.

b. Beilinson in combination with Freund and Arai fails to describe or suggest generating an approval user interface requesting authorization from the user to modify the prioritized user choice setting in accordance with the modification request received

Appellants again surmise that the Office admits Freund and Arai alone and in combination do not describe or suggest in response to the request from the application to modify the prioritized user choice setting, generating an approval user interface requesting authorization from the user to modify the prioritized user choice setting in accordance with the modification request received. The Office appears to allege Beilinson, at paragraph [0065], in combination with Freund and Arai describes or suggests this element.

Beilinson and Arai fail to remedy the deficiencies of Freund with respect to all elements of independent claim 19. Beilinson does not describe or suggest in response to the request from the application to modify the prioritized user choice setting, generating an approval user interface requesting authorization from the user to modify the prioritized user choice setting in accordance with the modification request received. Beilinson merely describes an administrator that restricts a user's logon hours, logon duration, access to computer functions, and access to applications based on content rating. At best, Beilinson

explains that an administrator may authorize a user's request for additional privileges. Beilinson fails to describe or suggest *(a)* receiving a modification to a protected user setting from the application that set the user setting and *(b)* in response to that request for a modification, generating an approval interface for the user that set the protected user setting to authorize the modification request. The approval interface provides user notification and user approval of changes to the protected values by the application. Freund, Beilinson, and Arai, alone and in combination, fail to describe or suggest in response to the request from the application to modify the prioritized user choice setting, generating an approval user interface requesting authorization from the user to modify the prioritized user choice setting in accordance with the modification request received.

B) U.S. Patent Publication No. 2004/0199763 ("Freund"), U.S. Patent Publication No. 2004/0003279 ("Beilinson"), U.S. Patent Publication No. 2004/0193606 ("Arai"), and U.S. Patent Publication No. 2002/0143961 ("Siegel") fail to render the invention of dependent claims 2-8, 10-11, 15-18, 20-25, and 28-29 obvious under 35 U.S.C. § 103(a) because Freund, Beilinson, Arai, and Siegel fails to describe or suggest, among other things, an operating system with a registry, wherein the protected value is a registry key stored in the registry, wherein the access control indicator is an access control list (ACL) that has been initialized to prevent writing to the protected value.

(i) Claims 2 and 20

It is respectfully submitted that the cited art, including Freund, Beilinson, Arai, and Siegel fails to describe or suggest, among other things, *wherein the computing device of the user has an operating system with a registry, wherein the protected value is a registry key stored in the registry, wherein the access control indicator is an access control list (ACL) that has been initialized to prevent writing to the protected value, and wherein modifying the access control indicator includes modifying the access control indicator to permit writing to the protected value*, as recited in dependent claims 2 and 20.

The Office relies upon Siegel, at paragraphs [0004], [0008], [0019]-[0020], and [0039] in combination with Freund, Beilinson, and Arai to render the invention of claims 2 and 20 unpatentable.

a. Siegel in combination with Freund, Beilinson, and Arai fail to describe or suggest computing device of the user has an operating system with a registry, wherein the protected value is a registry key stored in the registry

Appellants, based on the sparse record provided by the Office, surmise that the Office admits Freund, Beilinson, and Arai alone and in combination do not describe or suggest the computing device of the user has an operating system with a registry, wherein the protected value is a registry key stored in the registry. The Office appears to allege Siegel, at paragraphs [0004], [0008], [0019]-[0020], and [0039], in combination with Freund, Beilinson, and Arai describes or suggests this element.

Siegel describes protecting user profiles. The user views the profile and modifies various fields in the profile. The user may also specify different permissions for different grains of information within the user profile. For example, a first set of permissions may be associated with the entire user profile whereas a second set of permissions may be associated with a particular field in the user profile. Siegel fails to describe or suggest the elements of independent claims 1 and 19 discussed above. Accordingly, by reason of their dependence on independent claims 1 and 19, dependent claims 2 and 20 are believed to be in condition for allowance.

Siegel fails to describe a registry for an operating system that stores protected values associated with user settings for a first application. The user settings for the first application are registry keys. The user profile, as explained at paragraph [0022] of Siegel, includes favorite pizza, user name, address, telephone number. This does not fairly describe or

suggest a registry for an operating system, nor does it suggest a registry having protected values for user setting associated with a first application. Siegel in combination with Freund, Beilinson, and Arai fails to describe or suggest the computing device of the user has an operating system with a registry, wherein the protected value is a registry key stored in the registry.

b. Siegel in combination with Freund, Beilinson, and Arai fail to describe or suggest the access control indicator is an access control list (ACL) that has been initialized to prevent writing to the protected value, and wherein modifying the access control indicator includes modifying the access control indicator to permit writing to the protected value

Appellants, based on the sparse record provided by the Office, surmise that the Office admits Freund, Beilinson, and Arai alone and in combination do not describe or suggest the access control indicator is an access control list (ACL) that has been initialized to prevent writing to the protected value, and wherein modifying the access control indicator includes modifying the access control indicator to permit writing to the protected value. The Office appears to allege Siegel, at paragraphs [0004], [0008], [0019]-[0020], and [0039], in combination with Freund, Beilinson, and Arai describes or suggests this element.

Appellants further contend that Siegel does not fairly describe or suggest the access control indicator is an access control list (ACL) that has been initialized to prevent writing to the protected value, and wherein modifying the access control indicator includes modifying the access control indicator to permit writing to the protected value. Siegel, at paragraph [0033], describes permissions that specify the access rights, i.e., read, write, delete, etc for the user profile and fields of the user profile. Siegel, at paragraph [0038] also describes permission read and permission write controls. However, nothing in Siegel describe or suggests the access control list that prevents writing to the registry of the operating system.

Furthermore, Siegel fails to describe or suggest that modification to the access control indicator includes modifying the indicator to permit writing to the protected value. Siegel in combination with Freund, and Beilinson and Arai fails to describe or suggest the access control indicator is an access control list (ACL) that has been initialized to prevent writing to the protected value stored in the registry, and wherein modifying the access control indicator includes modifying the access control indicator to permit writing to the protected value.

(ii) Claims 3 and 21

It is respectfully submitted that the cited art, including Freund, Beilinson, Arai, and Siegel fails to describe or suggest, among other things, *wherein the operating system also includes a security subsystem, and wherein modifying the access control indicator to permit writing to the protected value includes providing to the user rights to modify the ACL in accordance with the security subsystem of the operating system,* as recited in dependent claims 3 and 21.

The Office relies upon Siegel, at paragraphs [0020] and [0026] in combination with Freund, Beilinson, and Arai to render the invention of claims 3 and 16unpatentable.

a. Siegel in combination with Freund, Beilinson, and Arai do not describe or suggest an operating system with a security subsystem

Appellants based on the sparse record provided by the Office surmise that the Office admits Freund, Beilinson, and Arai alone and in combination do not describe or suggest wherein the operating system also includes a security subsystem, and wherein modifying the access control indicator to permit writing to the protected value includes providing to the user rights to modify the ACL in accordance with the security subsystem of the operating system. The Office appears to allege Siegel, at paragraphs [0020] and [0026], in combination with Freund, Beilinson, and Arai describes or suggests this element.

Siegel describes protecting user profiles. The user views the profile and modifies various fields in the profile. The user may also specify different permissions for different grains of information within the user profile. For example, a first set of permissions may be associated with the entire user profile whereas a second set of permissions may be associated with a particular field in the user profile. The permissions specify the account-I.D. and access rights for each of the clients or groups that have access to the user profile, as explained by Siegel at paragraphs [0033]-[0034].

Siegel fails to describe an operating system also includes a security subsystem, and modifying the access control indicator to permit writing to the protected value includes providing to the user rights to modify the ACL in accordance with the security subsystem of the operating system. Siegel's system is very different from the invention of the claims because the user profile is owned by the user who views and modifies it. In the invention of the claims, the registry is owned by the operating system. This distinction is important as the operation of the invention varies drastically when providing access rights to the user settings for the first application stored as registry keys. For instance, the user profile as explained at paragraph [0026] and [0032]-[0034] of Siegel is managed by the user to provide permissions for clients and groups. In other words, the user manages the permissions for the user profile. Because the registry is not a user profile and is not owned by the user, the security subsystem must grant access rights to the user to allow modification of the registry values. Thus, the user management of a user profile as explained by Siegel does not fairly describe or suggest a security subsystem of the operating system neither does it suggest providing a user with rights to modify the registry keys maintained in the registry. Siegel in combination with Freund, Beilinson, and Arai fails to describe or suggest a security subsystem, and modifying the access

control indicator to permit writing to the protected value includes providing to the user rights to modify the ACL in accordance with the security subsystem of the operating system.

(iii) Claim 16

Freund, Beilinson, Arai, and Siegel, also, fail to describe or suggest, among other things, *wherein the computing device of the user includes an operating system having a security subsystem, and wherein the security subsystem modifies the ACL to permit the first application or another application to modify the user choice setting associated with the first application upon receiving user approval of the request to modify the user choice setting,* as recited in dependent claim 16.

The Office relies upon Siegel, at paragraphs [0020] and [0026] in combination with Freund, Beilinson, and Arai to render the invention of claim16 unpatentable.

a. Siegel in combination with Freund, Beilinson, and Arai fail to describe or suggest the computing device of the user includes an operating system having a security subsystem that modifies the ACL

Appellants, based on the sparse record provided by the Office, surmise that the Office admits Freund, Beilinson, and Arai alone and in combination do not describe or suggest wherein the computing device of the user includes an operating system having a security subsystem, and wherein the security subsystem modifies the ACL to permit the first application or another application to modify the user choice setting associated with the first application upon receiving user approval of the request to modify the user choice setting. The Office appears to allege Siegel, at paragraphs [0020] and [0026], in combination with Freund, Beilinson, and Arai describes or suggests this element.

Siegel fails to describe the computing device of the user includes an operating system having a security subsystem, and wherein the security subsystem modifies the ACL to

permit the first application or another application to modify the user choice setting associated with the first application upon receiving user approval of the request to modify the user choice setting. Siegel describes user management of permissions to the user profile having contact information and user food preferences. Siegel fails to describe or suggest user choice settings associated with a first application that are subject to a modification request by a first application or another application. Additionally, Siegel fails to describe or suggest the security subsystem that modifies the ACL in response to authorization received from a user.

Appellants further contend that Siegel does not fairly describe or suggest the first application or another application that request modification of the user choice setting or receiving authorization for a user to approve the modification requested by the first application or another application. Siegel, at paragraph [0026], describes a user that sets permissions that specify the access rights, i.e., read, write, delete, etc. for the user profile and fields of the user profile. However, nothing in Siegel describes or suggests the authorization of modification requests received from a first application or another application. Siegel in combination with Freund, Beilinson, and Arai fail to describe or suggest the computing device of the user includes an operating system having a security subsystem, and wherein the security subsystem modifies the ACL to permit the first application or another application to modify the user choice setting associated with the first application upon receiving user approval of the request to modify the user choice setting.

(iv) Claims 4, 17, and 22

It is respectfully submitted that the cited art, including Freund, Beilinson, Arai, and Siegel fails to describe or suggest, among other things, *wherein modifying the access control indicator to permit writing to the protected value includes providing to the user ownership of*

the registry key that the ACL secures, and wherein ownership of the registry key automatically provides to the user rights to modify the ACL in accordance with the security subsystem of the operating system, as recited in dependent claims 4, 17, and 22.

The Office relies upon Siegel, at paragraph [0026], in combination with Freund, Beilinson, and Arai to render the invention of claims 4, 17, and 22 unpatentable.

a. Siegel in combination with Freund, Beilinson, and Arai fail to describe or suggest modifying the access control indicator to permit writing to the protected value includes providing to the user ownership of the registry key

Appellants, based on the sparse record provided by the Office, surmise that the Office admits Freund, Beilinson, and Arai alone and in combination do not describe or suggest wherein modifying the access control indicator to permit writing to the protected value includes providing to the user ownership of the registry key that the ACL secures. The Office appears to allege Siegel, at paragraphs [0026], in combination with Freund, Beilinson, and Arai describes or suggests this element.

Siegel fails to describe an operating system modifying the access control indicator to permit writing to the protected value includes providing to the user ownership of the registry key that the ACL secures. Siegel's system is very different from the invention of the claims because the user profile is owned by the user who views and modifies it. In the invention of the claims, the registry is owned by the operating system. This distinction is important as the operation of the invention varies drastically when providing access rights to the user settings for the first application stored as registry keys. For instance, the user profile as explained at paragraph [0026] and [0032]-[0034] is managed by the user to provide permissions for clients and groups. Here, as required by dependent claims 4, 17, and 22 ownership of the registry is transferred from the security subsystem to the user. Because the

registry is not a user profile and is not owned by the user, the ownership of the various values associated with the settings for the applications of the operating system is changed to the user. Thus, the user management of a user profile as explained by Siegel does not fairly describe or suggest the transfer ownership neither does it suggest modifying the access indicators of the registry keys maintained in the registry. Siegel in combination with Freund, Beilinson, and Arai fails to describe or suggest modifying the access control indicator to permit writing to the protected value includes providing to the user ownership of the registry key that the ACL secures.

b. Siegel in combination with Freund, Beilinson, and Arai fail to describe or suggest ownership of the registry key automatically provides to the user rights to modify the ACL

Appellants, based on the sparse record provided by the Office, surmise that the Office admits Freund, Beilinson, and Arai alone and in combination do not describe or suggest wherein ownership of the registry key automatically provides to the user rights to modify the ACL in accordance with the security subsystem of the operating system. The Office appears to allege Siegel, at paragraphs [0026], in combination with Freund, Beilinson, and Arai describes or suggests this element.

Appellants contend that Siegel does not fairly describe or suggest ownership of the registry key automatically provides to the user rights to modify the ACL in accordance with the security subsystem of the operating system. Siegel, at paragraph [0026], describes a user that set permissions that specify the access rights, i.e., read, write, delete, etc. for the user profile and fields of the user profile. However, nothing in Siegel describes or suggests ownership of a registry key value associated with applications of an operating system. Furthermore, Siegel is silent regarding automatically providing write permissions to a user that

received ownership of a user profile field via a modification request. Siegel in combination with Freund, Beilinson, and Arai fails to describe or suggest ownership of the registry key automatically provides to the user rights to modify the ACL in accordance with the security subsystem of the operating system.

(v) Claims 5 and 23

It is respectfully submitted that the cited art, including Freund, Beilinson, Arai, and Siegel fails to describe or suggest, among other things, *wherein providing to the user ownership of the registry key that the ACL secures includes temporarily providing to the ownership of the registry key that the ACL secures,* as recited in dependent claims 5 and 23.

The Office relies upon Siegel, at paragraph [0026] in combination with Freund, Beilinson, and Arai to render the invention of claims 5 and 23 unpatentable.

a. Siegel in combination with Freund, Beilinson, and Arai fail to describe or suggest providing to the user ownership of the registry key that the ACL secures includes temporarily providing ownership of the registry key that the ACL secures

Appellants, based on the sparse record provided by the Office, surmise that the Office admits Freund, Beilinson, and Arai alone and in combination do not describe or suggest wherein providing to the user ownership of the registry key that the ACL secures includes temporarily providing ownership of the registry key that the ACL secures. The Office appears to allege Siegel, at paragraph [0026], in combination with Freund, Beilinson, and Arai describes or suggests this element.

Siegel fails to describe providing to the user ownership of the registry key that the ACL secures includes temporarily providing to the user ownership of the registry key that the ACL secures. Siegel does not describe temporary ownership of a user profile or fields for a user profile. In Siegel, the user profile is owned by the user who views and modifies it. In the

invention of the claims, the registry is owned by the operating system. This distinction is important as the operation of the invention varies drastically when providing access rights to the user settings for the first application stored as registry keys. For instance, the user profile as explained at paragraph [0026] and [0032]-[0034] is managed by the user to provide permissions for clients and groups. Here in the invention of claims 5 and 23, the user obtains temporary ownerships of the registry keys associated with the user choice settings. Because the registry is not a user profile and is not owned by the user, the security subsystem grants temporary user ownership to allow modification of the registry values. Thus, the user management of a user profile as explained by Siegel does not fairly describe or suggest the temporary ownership of the registry values for applications of an operating system. Siegel in combination with Freund, Beilinson, and Arai fail to describe or suggest providing to the user ownership of the registry key that the ACL secures includes temporarily providing to the user ownership of the registry key that the ACL secures.

(vi) Claim18

Freund, Beilinson, Arai, and Siegel, also, fail to describe or suggest, among other things, *wherein the security subsystem modifies the ACL to permit writing to the protected value in the registry key includes by providing to the user temporary ownership of the registry key, wherein temporary ownership of the registry key automatically provides to the user rights to temporarily modify the ACL in accordance with the security subsystem of the operating system,* as recited in dependent claim 18.

The Office relies upon Siegel, at paragraph [0026] in combination with Freund, Beilinson, and Arai to render the invention of claim 18 unpatentable.

a. Siegel in combination with Freund, Beilinson, and Arai fail to describe or suggest the security subsystem modifies the ACL to permit writing to

the protected value in the registry key includes by providing to the user temporary ownership of the registry key

Appellants, based on the sparse record provided by the Office, surmise that the Office admits Freund, Beilinson, and Arai alone and in combination do not describe or suggest wherein the security subsystem modifies the ACL to permit writing to the protected value in the registry key includes by providing to the user temporary ownership of the registry key, wherein temporary ownership of the registry key automatically provides to the user rights to temporarily modify the ACL in accordance with the security subsystem of the operating system. The Office appears to allege Siegel, at paragraph [0026], in combination with Freund, Beilinson, and Arai describes or suggests this element.

Appellants further contend that Siegel does not fairly describe or suggest the security subsystem modifies the ACL to permit writing to the protected value in the registry key includes by providing to the user temporary ownership of the registry key, wherein temporary ownership of the registry key automatically provides to the user rights to temporarily modify the ACL in accordance with the security subsystem of the operating system. Siegel, at paragraph [0026], describes a user that set permissions that specify the access rights, i.e., read, write, delete, etc. for the user profile and fields of the user profile. However, nothing in Siegel describe or suggests the allowing temporary user ownership automatically provide temporary write permissions for a registry of the operating system. Siegel fails to describe or suggest user rights to temporarily modify the ACL in accordance with the security subsystem of the operating system. Siegel in combination with Freund, Beilinson, and Arai fail to describe or suggest the security subsystem modifies the ACL to permit writing to the protected value in the registry key includes by providing to the user temporary ownership of the registry key, wherein temporary ownership of the registry key

automatically provides to the user rights to temporarily modify the ACL in accordance with the security subsystem of the operating system.

(vii) Claim 6

It is respectfully submitted that the cited art, including Freund, Beilinson, Arai, and Siegel fails to describe or suggest, among other things, *wherein securing the prioritized user choice setting as a protected value using the access control indicator includes securing the prioritized user choice setting as a protected value using the access control indicator to prohibit the second application from writing to the protected value, and wherein modifying the access control indicator to permit modification of the prioritized user choice setting associated with the first application to be consistent with the modification request received from the second application includes modifying the access control indicator to permit the second application to write to the protected value,* as recited in dependent claim 6.

The Office relies upon Siegel, at paragraph [0026] in combination with Freund, at paragraph [0023], Beilinson, and Arai to render the invention of claim 6 unpatentable.

a. Siegel in combination with Freund, Beilinson, and Arai fail to describe or suggest securing the prioritized user choice setting as a protected value using the access control indicator to prohibit the second application from writing to the protected value

Appellants, based on the sparse record provided by the Office, surmise that the Office admits Freund, Beilinson, and Arai alone and in combination do not describe or suggest wherein securing the prioritized user choice setting as a protected value using the access control indicator includes securing the prioritized user choice setting as a protected value using the access control indicator to prohibit the second application from writing to the protected value. The Office appears to allege Siegel, at paragraph [0026], in combination with Freund, Beilinson, and Arai describes or suggests this element.

Siegel fails to describe securing the prioritized user choice setting as a protected value using the access control indicator includes securing the prioritized user choice setting as a protected value using the access control indicator to prohibit the second application from writing to the protected value. Siegel does not describe a second application of an operating system that is prohibited from writing to a protected and secured registry value. In Siegel, the user profile is owned by the user who views and modifies it. The use profile stores information about a user and not data regarding operation of an application of the operating system. For instance, the user profile as explained at paragraph [0026] and [0032]-[0034] is managed by the user to provide permissions for clients and groups. Here in the invention of claim 6, the second application is prohibited from modifying registry values stored by the registry. The user profile sets permissions for clients and not applications of an operating system. The Office alleges that it is *inherent* that once a user or administrator is done modifying the profile, the user or administrator will log out and the profile will be protected from modifications until another party is verified or authenticated. The Office concludes that a feature of claim 6 is inherent without showing via rationale or evidence that this feature is inherent. See MPEP 2112. The record is devoid of any reasoning or technical evidence to show that claim 6 or securing the prioritized user choice setting as a protected value using the access control indicator includes securing the prioritized user choice setting as a protected value using the access control indicator to prohibit the second application from writing to the protected value is inherent. A user logging out of a system does not prevent an application associated with the operating system from changing registry values. A user logging out does not describe or suggest a access control indicator that prohibits a second application from writing to a protected registry value. Siegel in combination with Freund, Beilinson, and Arai fails to

describe or suggest securing the prioritized user choice setting as a protected value using the access control indicator includes securing the prioritized user choice setting as a protected value using the access control indicator to prohibit the second application from writing to the protected value.

b. Freund in combination with Siegel, Beilinson, and Arai fails to describe or suggest modifying the access control indicator to permit the second application to write to the protected value

Appellants, based on the sparse record provided by the Office, surmise that the Office admits Siegel, Beilinson, and Arai alone and in combination do not describe or suggest wherein modifying the access control indicator to permit modification of the prioritized user choice setting associated with the first application to be consistent with the modification request received from the second application includes modifying the access control indicator to permit the second application to write to the protected value. The Office appears to allege Freund, at paragraph [0023], in combination with Siegel, Beilinson, and Arai describes or suggests this element.

Appellants further contend that Freund does not fairly describe or suggest modifying the access control indicator to permit modification of the prioritized user choice setting associated with the first application to be consistent with the modification request received from the second application includes modifying the access control indicator to permit the second application to write to the protected value. Freund, at paragraph [0023], describes a process communication policy that prohibits one process from communicating with another process. However, nothing in Freund describes or suggests allowing a second application to modify user choice settings stored in the registry. Freund fails to describe or suggest the user choice settings are associated with a first application. Freund in combination with Siegel,

Beilinson, and Arai fail to describe or suggest modifying the access control indicator to permit modification of the prioritized user choice setting associated with the first application to be consistent with the modification request received from the second application includes modifying the access control indicator to permit the second application to write to the protected value.

(viii) Claim 7

It is respectfully submitted that the cited art, including Freund, Beilinson, Arai, and Siegel fails to describe or suggest, among other things, *wherein restoring the access control indicator to prohibit further modification by the second application includes returning ownership of the registry key value that the ACL secures to the operating system,* as recited in dependent claim 7.

The Office relies upon Siegel, at paragraph [0026] in combination with Freund, Beilinson, and Arai to render the invention of claim 7 unpatentable.

a. Siegel in combination with Freund, Beilinson, and Arai fail to describe or suggest restoring the access control indicator to prohibit further modification by the second application includes returning ownership of the registry key value that the ACL secures to the operating system

Appellants, based on the sparse record provided by the Office, surmise that the Office admits Freund, Beilinson, and Arai alone and in combination do not describe or suggest wherein restoring the access control indicator to prohibit further modification by the second application includes returning ownership of the registry key value that the ACL secures to the operating system. The Office appears to allege Siegel, at paragraph [0026], in combination with Freund, Beilinson, and Arai describes or suggests this element.

As discussed extensively above, Siegel describes protecting user profiles. The user views the profile and modifies various fields in the profile.

Siegel fails to describe restoring the access control indicator to prohibit further modification by the second application includes returning ownership of the registry key value that the ACL secures to the operating system. Siegel does not describe temporary ownership of a user profile or fields for a user profile. In Siegel, the user profile is owned by the user who views and modifies it. In the invention of the claims, the registry is owned by the operating system. This distinction is important as the operation of the invention varies drastically when providing access rights to the user settings for the first application stored as registry keys. For instance, the user profile as explained at paragraph [0026] and [0032]-[0034] is managed by the user to provide permissions for clients and groups. Here in the invention of claim 7, the temporary ownership by the user is returned to the operating system to prevent modification of the registry keys associated with the protected user choice settings. Because the registry is not a user profile and is not owned by the user, the operating system ownership is restored to prevent modification of the registry values. Thus, the user management of a user profile as explained by Siegel does not fairly describe or suggest restoring ownership of the registry values for applications of an operating system. Siegel in combination with Freund, Beilinson, and Arai fails to describe or suggest restoring the access control indicator to prohibit further modification by the second application includes returning ownership of the registry key value that the ACL secures to the operating system.

Furthermore, the Office alleges that it is *inherent* that once a user or administrator is done modifying the profile, the user or administrator will log out and the profile will be protected from modifications until another party is verified or authenticated. The Office concludes that a feature of claim 7 is inherent without showing via rationale or evidence that this feature is inherent. See MPEP 2112. The record is devoid of any reasoning

or technical evidence to show that claim 7 or returning ownership of the registry key value that the ACL secures to the operating system is inherent when prohibiting access by the second application of the operating system or prohibiting access to the promised user choice setting stored in the registry of the operating system. A user logging out of a system does not prevent and operating system from modifying registry values. Furthermore, a user is not an application that is prohibited from modifying the registry values.

(ix) Claim 25

Freund, Beilinson, Arai, and Siegel also fails to describe or suggest, among other things, *wherein restoring the access control indicator to prohibit further modification of the prioritized user choice setting includes returning ownership of the registry key value that the ACL secures to the operating system,* as recited in dependent claim 25.

The Office relies upon Siegel, at paragraph [0026] in combination with Freund, Beilinson, and Arai to render the invention of claim 25 unpatentable.

a. Siegel, at paragraph [0026], in combination with Freund, Beilinson, and Arai fail to describe or suggest restoring the access control indicator to prohibit further modification of the prioritized user choice setting includes returning ownership of the registry key value that the ACL secures to the operating system

Appellants, based on the sparse record provided by the Office, surmise that the Office admits Freund, Beilinson, and Arai alone and in combination do not describe or suggest wherein restoring the access control indicator to prohibit further modification of the prioritized user choice setting includes returning ownership of the registry key value that the ACL secures to the operating system. The Office appears to allege Siegel, at paragraph [0026], in combination with Freund, Beilinson, and Arai describes or suggests this element.

Appellants further contend that Siegel does not fairly describe or suggest restoring the access control indicator to prohibit further modification of the prioritized user choice setting includes returning ownership of the registry key value that the ACL secures to the operating system. Siegel, at paragraph [0026], describes a user that set permissions that specify the access rights, i.e., read, write, delete, etc. for the user profile and fields of the user profile. However, nothing in Siegel describe or suggests the restoring ownership to the operating system prohibits modification of the registry values associated with a first application of the operating system. Siegel fails to describe or suggest preventing modification of registry values of an operating system. Siegel in combination with Freund, Beilinson, and Arai fail to describe or suggest restoring the access control indicator to prohibit further modification of the prioritized user choice setting includes returning ownership of the registry key value that the ACL secures to the operating system.

(x) Claim 24

It is respectfully submitted that the cited art, including Freund, Beilinson, Arai, and Siegel fails to describe or suggest, among other things, *wherein modifying the access control indicator to permit modification of the prioritized user choice setting associated with the application to be consistent with the modification request received includes requiring user to modify the access control indicator to permit writing to the protected value in accordance with the security subsystem of the operating system,* as recited in dependent claim 24.

The Office relies upon Siegel, at paragraph [0026] in combination with Freund, Beilinson, and Arai to render the invention of claim 24 unpatentable.

a. Siegel in combination with Freund, Beilinson, and Arai fail to describe or suggest modifying the access control indicator to permit modification of the prioritized user choice setting associated with the application to be consistent with the modification request received includes requiring

a user to modify the access control indicator to permit writing to the protected value in accordance with the security subsystem of the operating system

Appellants, based on the sparse record provided by the Office, surmise that the Office admits Freund, Beilinson, and Arai alone and in combination do not describe or suggest wherein modifying the access control indicator to permit modification of the prioritized user choice setting associated with the application to be consistent with the modification request received includes requiring a user to modify the access control indicator to permit writing to the protected value in accordance with the security subsystem of the operating system. The Office appears to allege Siegel, at paragraph [0026], in combination with Freund, Beilinson, and Arai describes or suggests this element.

Siegel fails to describe wherein modifying the access control indicator to permit modification of the prioritized user choice setting associated with the application to be consistent with the modification request received includes requiring the user to modify the access control indicator to permit writing to the protected value in accordance with the security subsystem of the operating system. Siegel does not describe an application of an operating system that request modification of a protected and secured registry value. In Siegel, the user profile is owned by the user who views and modifies it. The use profile stores information about a user and not data regarding operation of an application of the operating system. For instance, the user profile as explained at paragraph [0026] and [0032]-[0034] is managed by the user to provide permissions for clients and groups. Here in the invention of claim 24, the modification to the access control indicators requested by the application is prohibited unless the user modifies the access control indicator for the registry values. The user profile set permissions for clients and not applications of an operating system. Siegel in combination with Freund, Beilinson, and Arai fails to describe or suggest modifying the access control indicator

to permit modification of the prioritized user choice setting associated with the application to be consistent with the modification request received includes requiring user to modify the access control indicator to permit writing to the protected value in accordance with the security subsystem of the operating system.

Appellants further contend that Siegel does not fairly describe or suggest user modification of the access control indicator associated with a registry value of the operating system to permit modification of the prioritized user choice setting associated with the application. Siegel, at paragraph [0026], describes setting user profile permission. However, nothing in Siegel describes or suggests allowing an application to modify user choice settings stored in registry. Siegel fails to describe or suggest the user choice settings are associated with an application. Siegel in combination with Freund, Beilinson, and Arai fail to describe or suggest modifying the access control indicator to permit modification of the prioritized user choice setting associated with the application to be consistent with the modification request received includes requiring user to modify the access control indicator to permit writing to the protected value in accordance with the security subsystem of the operating system.

Furthermore, the Office alleges that it is *inherent* that once a user or administrator is done modifying the profile, the user or administrator will log out and the profile will be protected from modifications until another party is verified or authenticated. The Office concludes that a feature of claim 24 is inherent without showing via rationale or evidence that this feature is inherent. See MPEP 2112. The record is devoid of any reasoning or technical evidence to show that claim 24 or modifying the access control indicator to permit modification of the prioritized user choice setting associated with the application to be consistent with the modification request received includes requiring the user to modify the

access control indicator to permit writing to the protected value of registry in accordance with the security subsystem of the operating system. A user logging out of a system does not describe or suggest user modification of an access control indicator associated with a registry of the operating system. Furthermore, authentication and verification of a user fails to suggest modifying the access control indicator to permit writing to the protected value of the registry.

(xi) Claim 8

It is respectfully submitted that the cited art, including Freund, Beilinson, Arai, and Siegel fails to describe or suggest, among other things, *displaying, in association with the approval user interface, the prioritized user choice setting along with options for modifying the prioritized user choice setting, wherein receiving input from the user approving the modification of the prioritized user choice setting comprises receiving input from the user in accordance with at least one of the displayed options,* as recited in dependent claim 8.

The Office relies upon Siegel, at paragraph [0026] in combination with Freund, Beilinson, at paragraph [0065], and Arai to render the invention of claim 8 unpatentable.

a. Siegel in combination with Freund, Beilinson, and Arai fails to describe or suggest displaying, in association with the approval user interface, the prioritized user choice setting along with options for modifying the prioritized user choice set

Appellants, based on the sparse record provided by the Office, surmise that the Office admits Freund, Beilinson, and Arai alone and in combination do not describe or suggest displaying, in association with the approval user interface, the prioritized user choice setting along with options for modifying the prioritized user choice setting. The Office appears to allege Siegel, at paragraph [0026], in combination with Freund, Beilinson, and Arai describes or suggests this element.

Siegel fails to describe displaying, in association with the approval user interface, the prioritized user choice setting along with options for modifying the prioritized user choice setting. Siegel does not describe the prioritized user choice setting for a registry of the operating system and options for modifying the user choice settings are displayed in an approval user interface. In Siegel, the user profile is managed by the user. In the invention of claim 8, the registry values are stored and require express approval of the user before modifications are made. The user profile as explained at paragraph [0026] and [0032]-[0034] is managed by the user to provide various permissions for clients and groups before modifications are made. Here in the invention of claim 8, the user grants a modifications and implements the requested modifications. Because the registry is not a user profile, the modifications to the registry values require approval. Siegel in combination with Freund, Beilinson, and Arai fails to describe or displaying, in association with the approval user interface, the prioritized user choice setting along with options for modifying the prioritized user choice setting.

b. <u>Beilinson in combination with Siegel, Freund, and Arai fails to describe or suggest receiving input from the user approving the modification of the prioritized user choice setting comprises receiving input from the user in accordance with at least one of the displayed options</u>

Appellants, based on the sparse record provided by the Office, surmise that the Office admits Siegel, Freund, and Arai alone and in combination do not describe or suggest wherein receiving input from the user approving the modification of the prioritized user choice setting comprises receiving input from the user in accordance with at least one of the displayed options. The Office appears to allege Beilinson, at paragraph [0065], in combination with Siegel, Freund, and Arai describes or suggests this element.

Appellants further contend that Siegel does not fairly wherein receiving input from the user approving the modification of the prioritized user choice setting comprises receiving input from the user in accordance with at least one of the displayed options. Beilinson, at paragraph [0065], describes a wizard that sets access rights. An administrator may prohibit access to applications of the computer system. In turn, a user may request temporary increases in access privileges. The access privileges are not registry values of a first application and do not correspond to changes of those values by a second application. Furthermore, nothing in Beilinson describes or suggests receiving modification input from the user approving a modification to the registry values associated with the first application and requested by the second application. Beilinson in combination with Siegel, Freund, and Arai fail to describe or suggest receiving input from the user approving the modification of the prioritized user choice setting comprises receiving input from the user in accordance with at least one of the displayed options.

(xii) Claims 10 and 28

It is respectfully submitted that the cited art, including Freund, Beilinson, Arai, and Siegel fails to describe or suggest, among other things, *wherein the prioritized user choice setting includes at least one of a user preference relating to a file association, an autoplay setting, contents of a start menu, a registered client setting, a protocol handler, a MIME type handler, a task association, a Web browser home page, a reset Web page setting, and a sidebar setting,* as recited in dependent claims 10 and 28.

The Office relies upon Siegel, at paragraph [0004], in combination with Freund, Beilinson, and Arai to render the invention of claims 10 and 28 unpatentable.

a. Siegel in combination with Freund, Beilinson, and Arai fail to describe or suggest prioritized user choice setting includes at least one of a user

preference relating to a file association, an autoplay setting, contents of a start menu, a registered client setting, a protocol handler, a MIME type handler, a task association, a Web browser home page, a reset Web page setting, and a sidebar setting

Appellants, based on the sparse record provided by the Office, surmise that the Office admits Freund, Beilinson, and Arai alone and in combination do not describe or suggest wherein the prioritized user choice setting includes at least one of a user preference relating to a file association, an autoplay setting, contents of a start menu, a registered client setting, a protocol handler, a MIME type handler, a task association, a Web browser home page, a reset Web page setting, and a sidebar setting. The Office appears to allege Siegel, at paragraph [0004], in combination with Freund, Beilinson, and Arai describes or suggests this element.

Siegel fails to describe wherein the prioritized user choice setting includes at least one of a user preference relating to a file association, an autoplay setting, contents of a start menu, a registered client setting, a protocol handler, a MIME type handler, a task association, a Web browser home page, a reset Web page setting, and a sidebar setting. In Siegel, the user profile is owned by the user who views and modifies it. In the invention of the claims, the registry is associated with the operating system and not the user. This distinction is important as the operation of the invention varies drastically when providing access rights to the user settings for the first application stored as registry keys. Here in the invention of claims 10 and 28, the user specifies registry settings for a file association, an autoplay setting, contents of a start menu, a registered client setting, a protocol handler, a MIME type handler, a task association, a Web browser home page, a reset Web page setting, and a sidebar setting. Siegel is silent regarding registry settings for a file association. Siegel is silent regarding registry settings for an autoplay setting. Siegel is silent regarding registry settings for contents of a start menu. Siegel is silent regarding registry settings for a registered client setting. Siegel is

silent regarding registry settings for a protocol handler. Siegel is silent regarding registry settings for a MIME type handler. Siegel is silent regarding registry settings for a task association. Siegel is silent regarding registry settings for a Web browser home page. Siegel is silent regarding registry settings for a reset Web page setting. These registry settings are modified by an application in accordance with user approval of the received modifications to the registry settings. Siegel in combination with Freund, Beilinson, and Arai fails to describe or suggest wherein the prioritized user choice setting includes at least one of a user preference relating to a file association, an autoplay setting, contents of a start menu, a registered client setting, a protocol handler, a MIME type handler, a task association, a Web browser home page, a reset Web page setting, and a sidebar setting.

Appellants further contend that Siegel does not fairly describe or suggest the user choice settings stored in a registry of an operating system as protected values. Siegel, at paragraph [0004], describes a user that set permissions, which specify the access rights, i.e., read, write, delete, etc. for the user profile and fields of the user profile. However, nothing in Siegel describe or suggests wherein the protected and prioritized user choice setting includes at least one of a user preference relating to a file association, an autoplay setting, contents of a start menu, a registered client setting, a protocol handler, a MIME type handler, a task association, a Web browser home page, a reset Web page setting, and a sidebar setting.

(xiii) Claim 11, 15, and 29

It is respectfully submitted that the cited art, including Freund, Beilinson, Arai, and Siegel fails to describe or suggest, among other things, *wherein the prioritized user choice setting includes the registered client setting, and wherein the registered client setting includes*

at least one of a Web browser, e-mail, media player, instant messaging, and virtual machine for Java setting, as recited in dependent claims 11, 15, and 29.

The Office relies upon Siegel, at paragraph [0026], in combination with Freund, Beilinson, and Arai to render the invention of claims 11, 15, and 29 unpatentable.

a. Siegel in combination with Freund, Beilinson, and Arai fail to describe or suggest prioritized user choice setting includes the registered client setting, and wherein the registered client setting includes at least one of a Web browser, e-mail, media player, instant messaging, and virtual machine for Java setting

Appellants, based on the sparse record provided by the Office, surmise that the Office admits Freund, Beilinson, and Arai alone and in combination do not describe or suggest wherein the prioritized user choice setting includes the registered client setting, and wherein the registered client setting includes at least one of a Web browser, e-mail, media player, instant messaging, and virtual machine for Java setting. The Office appears to allege Siegel, at paragraph [0026], in combination with Freund, Beilinson, and Arai describes or suggests this element.

Siegel fails to describe wherein the prioritized user choice setting includes the registered client setting, and wherein the registered client setting includes at least one of a Web browser, e-mail, media player, instant messaging, and virtual machine for Java setting. In the invention of the claims, the registry is associated with the operating system and not the user. This distinction is important as the operation of the invention varies drastically when providing access rights to the user settings for the first application stored as registry keys. Here in the invention of claims 11, 15, and 29, the user specifies registry settings that include the registered client setting, and wherein the registered client setting includes at least one of a Web browser, e-mail, media player, instant messaging, and virtual machine for Java setting. Siegel

is silent regarding a registered client setting. Siegel is silent regarding a Web browser setting. Siegel is silent regarding an e-mail setting. Siegel is silent regarding a media player setting. Siegel is silent regarding an instant messaging setting. Siegel is silent regarding virtual machine for Java setting. These registry settings are modified by an application in accordance with user approval of the received modifications to the registry settings. Siegel in combination with Freund, Beilinson, and Arai fails to describe or suggest the prioritized user choice setting includes the registered client setting, and wherein the registered client setting includes at least one of a Web browser, e-mail, media player, instant messaging, and virtual machine for Java setting.

Appellants further contend that Siegel does not fairly describe or suggest a registry of the operating system storing the protected settings. Siegel, at paragraph [0026], describes a web browser is utilized to view a user profile. However, nothing in Siegel describes or suggests the protected registry values of an operating system for a first application are prioritized user choice setting that include the registered client setting, and wherein the registered client setting includes at least one of a Web browser, e-mail, media player, instant messaging, and virtual machine for Java setting.

C) U.S. Patent Publication No. 2004/0199763 ("Freund"), U.S. Patent Publication No. 2004/0003279 ("Beilinson"), U.S. Patent Publication No. 2004/0193606 ("Arai"), U.S. Patent Publication No. 2002/0143961 ("Siegel"), and U.S. Patent No. 6,370,141 ("Giordano III") fail to render the invention of dependent claims 9, 13, and 27 obvious under 35 U.S.C. § 103(a) because Freund, Beilinson, Arai, Siegel, and Giordano III fail to describe or suggest notification of when the prioritized user choice setting has been modified, the notification identifying the application and the prioritized user choice setting before and after the modification .

(i) Claims 9 and 27

It is respectfully submitted that the cited art, including Freund, Beilinson, Arai, Siegel, and Giordano III fails to describe or suggest, among other things, *generating a change*

notification when the prioritized user choice setting has been modified, the change notification identifying the second application and the prioritized user choice setting before and after the modification and the change notification identifies the application, as recited in dependent claims 9 and 27.

The Office relies upon Giordano III, at col. 4, ll. 15-24, in combination with Freund, Beilinson, Arai, and Siegel to render the invention of claims 9 and 27 unpatentable.

a. Giordano III in combination with Freund, Beilinson, Arai, and Siegel fail to describe or suggest generating a change notification when the prioritized user choice setting has been modified, the change notification identifying the second application and the prioritized user choice setting before and after the modification and the change notification identifies the application

Appellants, based on the sparse record provided by the Office, surmise that the Office admits Freund, Beilinson, Arai, and Siegel alone and in combination do not describe or suggest generating a change notification when the prioritized user choice setting has been modified, the change notification identifying the second application and the prioritized user choice setting before and after the modification and the change notification identifies the application. The Office appears to allege Giordano III, at col. 4, ll. 15-24, in combination with Freund, Beilinson, Arai, and Siegel describes or suggests this element.

Giordano III describes pushing setting changes to a device. The device, e.g. telephone periodically queries a web page for setting changes. The user receives a notification when the options are changed on the web page. In turn, the telephone is updated with the configuration changes. Giordano III fails to describe generating a change notification when the prioritized user choice setting has been modified, the change notification identifying the second application and the prioritized user choice setting before and after the modification and the change notification identifies the application. In the invention of claims 9 and 27, the registry

is associated with the operating system and not a telephone. This distinction is important as the operation of the invention varies drastically when generating notifications for changes made by a second application to registry values associated with a first application. Here in the invention of claims 9 and 27, the change notification received by the user includes the changes to registry settings and the application that is requesting the changes. In one embodiment, the application that requests the change and the application that set the changes are different. Giordano III is silent regarding showing in a notification the values of the setting before and after the modification. Giordano III in combination with Freund, Beilinson, Arai, and Siegel fails to describe or suggest a generating change notification when the prioritized user choice setting has been modified, the change notification identifying the second application and the prioritized user choice setting before and after the modification and the change notification identifies the application that set the registry values for the operating system.

Appellants further contend that Giordano III does not fairly describe or suggest the modifications in the notification are for registry settings for a first application different from the application requesting the change or the same as the application requesting the change. Giordano III describes generating a notification for device updates and updating device settings based on a webpage. However, nothing in Giordano III describes or suggests generating change notification when the prioritized user choice setting has been modified, the change notification identifying the second application and the prioritized user choice setting before and after the modification and the change notification identifies the application that set the registry values for the operating system.

(ii) Claim 13

It is respectfully submitted that the cited art, including Freund, Beilinson, Arai, Siegel, and Giordano III fails to describe or suggest, among other things, *wherein the approval user interface restores the ACL to prevent writing to the protected value in the registry key after writing the modified user choice setting, and wherein the approval user interface notifies the user whenever the approval user interface writes to the protected value, including notifying the user of a content of the protected value before and after the approval user interface writes to the protected value and an identity of the application that requested the modification,* as recited in dependent claim 13.

The Office relies upon Giordano III, at col. 4, ll. 15-24, in combination with Freund, Beilinson, at paragraph [0065], Arai, and Siegel to render the invention of claim 13 unpatentable.

a. Giordano III in combination with Freund, Beilinson, Arai, and Siegel fail to describe or suggest generating the approval user interface restores the ACL to prevent writing to the protected value in the registry key after writing the modified user choice setting, and wherein the approval user interface notifies the user whenever the approval user interface writes to the protected value, including notifying the user of a content of the protected value before and after the approval user interface writes to the protected value and an identity of the application that requested the modification

Appellants based on the sparse record provided by the Office surmise that the Office admits Freund, Arai, and Siegel alone and in combination do not describe or suggest wherein the approval user interface restores the ACL to prevent writing to the protected value in the registry key after writing the modified user choice setting, and wherein the approval user interface notifies the user whenever the approval user interface writes to the protected value, including notifying the user of a content of the protected value before and after the approval

user interface writes to the protected value and an identity of the application that requested the modification. The Office appears to allege Giordano III, at col. 4, ll. 15-24, in combination with Freund, Beilinson, at paragraph [0065], Arai, and Siegel describes or suggests this element.

Giordano III describes pushing setting changes to a device. The device, e.g. telephone periodically queries a web page for setting changes. The user receives notification when the options are changed on the web page. In turn, the telephone is updated with the configuration changes. Giordano III and Beilinson fails to describe wherein the approval user interface restores the ACL to prevent writing to the protected value in the registry key after writing the modified user choice setting, and wherein the approval user interface notifies the user whenever the approval user interface writes to the protected value, including notifying the user of content of the protected value before and after the approval user interface writes to the protected value and an identity of the application that requested the modification. In the invention of claim 13, the approval interface restores the ACL of the modified user choice setting in a registry associated with the operating system. This distinction is important as the operation of the invention varies drastically the when approval interface for changes to the registry settings include values before and after modification. Here in the invention of claim 13, the notification received by the user is part of an approval interface that includes the changes to registry settings and identifies the application that is requesting the changes to the registry values. Giordano III is silent regarding showing in the approval interface the values of the setting before and after the modification. Giordano III in combination with Freund, Beilinson, Arai, and Siegel fails to describe or suggest wherein the approval user interface restores the ACL to prevent writing to the protected value in the registry key after writing the

modified user choice setting, and wherein the approval user interface notifies the user whenever the approval user interface writes to the protected value.

Appellants further contend that Giordano III and Beilinson do not fairly describe or suggest the notifications include before and after values for registry settings for a first application different and the notifications are part of the approval interface provided to the user. Giordano III describes generating a notification for device updates and updating device settings based on a webpage. Beilinson describes generating an approval interface to increase user privileges. However, nothing in Giordano III and Beilinson describes or suggests an approval interface that prohibits further modification of the modified value and includes a notification identifying the application that modified the setting and the contents of the modified setting before and after the modification.

D) Claim 19 and its dependent claims are statutory subject matter under 35 U.S.C. § 101 because the Office failed to meet its burden of showings that at the time the invention was made one of ordinary skill in the art would understand that computer-accessible storage media was something other than a storage device, like computer memory.

Contrary to the Office's allegation, claims 19-25 and 27-29 are statutory subject matter. Appellants' specification explains that one of ordinary skill in the art understands that a memory stores data for a computing device. Further, a skilled artisan would interpret a computer-accessible storage medium to be a storage memory. Nothing in Appellants' specifications or claims recite a signal. Instead, claim 19 is a Beauregard claim that is patent eligible subject matter. See In re Beauregard, 53 F.3d 1583 (Fed. Cir. 1995). The record is devoid of any evidence that, at the time of the invention, the plain and ordinary meaning of computer-accessible storage medium included signals. Phillips v. AWH Corp., 415 F.3d 1303, 1313 (Fed. Cir. 2005) (the ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the

invention, *i.e.*, as of the effective filing date of the patent application.) The record is devoid of any evidence that as of the effective filing date of the patent application, the ordinary and customary meaning of computer-readable storage medium is a signal. The meaning of computer-readable storage medium to a person of ordinary skill in the art in question at the time of the invention, *i.e.*, as of the effective filing date of the patent application, is a storage memory device as explained by at least pages 4 and 11 of the Appellants original specification.

Accordingly, Appellants respectfully request withdrawal of the 35 U.S.C. § 101 rejection and allowance of independent claims 19-25 and 27-29

Appellants respectfully submit that the pending claims are in condition for allowance. As such, Appellants respectfully request that the rejection of the claims be reversed and that a timely Notice of Allowance be issued in this case. Should there be any unresolved matters, please contact the undersigned.

Respectfully submitted,

/MONPLAISIR HAMILTON/

Monplaisir Hamilton
Reg. No. 54,851

SHOOK, HARDY, & BACON L.L.P.
2555 Grand Blvd.
Kansas City, MO 64108-2613
Tel.: 816/474-6550
Fax: 816/421-5547
Attorney Docket No. MFCP.143750

VIII. CLAIMS APPENDIX

1. (Previously Presented) A method for prioritizing user application preferences based on user input data, the method comprising:

recognizing, at a computing device of a user, user input data relevant to a first application as a prioritized user choice setting associated with the first application, wherein the prioritized user choice setting determines at least one property of execution of at least one event of the first application;

securing, at the computing device of the user, the user choice setting as a protected value using an access control indicator, wherein the access control indicator prohibits a second application from modifying the prioritized user choice setting associated with the first application without authorization from the user;

receiving, at the computing device of the user, a request from the second application to modify the prioritized user choice setting associated with the first application;

in response to receiving the request from the second application to modify the prioritized user choice setting associated with the first application, generating an approval user interface on the computing device of the user, the approval user interface requesting authorization from the user to modify the prioritized user choice setting associated with the first application to be consistent with the modification request received from the second application;

receiving, at the computing device of the user, input from the user approving the modification of the prioritized user choice setting associated with

the first application to be consistent with the modification request received from the second application;

modifying, at the computing device of the user, the access control indicator to permit modification of the prioritized user choice setting associated with the first application to be consistent with the modification request received from the second application;

modifying, at the computing device of the user, the prioritized user choice setting to a different value in accordance with the received user input; and

restoring, at the computing device of the user, the access control indicator to prohibit further modification by the second application of the prioritized user choice setting associated with the first application.

2. (Previously Presented) The method of Claim 1,

wherein the computing device of the user has an operating system with a registry,

wherein the protected value is a registry key stored in the registry,

wherein the access control indicator is an access control list (ACL) that has been initialized to prevent writing to the protected value,

and wherein modifying the access control indicator includes modifying the access control indicator to permit writing to the protected value.

3. (Previously Presented) The method of Claim 2, wherein the operating system also includes a security subsystem, and wherein modifying the access control indicator to permit writing to the protected value includes providing to the user rights to modify the ACL in accordance with the security subsystem of the operating system.

4. (Previously Presented) The method of Claim 3, wherein modifying the access control indicator to permit writing to the protected value includes providing to the user ownership of the registry key that the ACL secures, and wherein ownership of the registry key automatically provides to the user rights to modify the ACL in accordance with the security subsystem of the operating system.

5. (Previously Presented) The method of Claim 4, wherein providing to the user ownership of the registry key that the ACL secures includes temporarily providing to the ownership of the registry key that the ACL secures.

6. (Previously Presented) The method of Claim 3,

wherein securing the prioritized user choice setting as a protected value using the access control indicator includes securing the prioritized user choice setting as a protected value using the access control indicator to prohibit the second application from writing to the protected value,

and wherein modifying the access control indicator to permit modification of the prioritized user choice setting associated with the first application to be consistent with the modification request received from the second application includes modifying the access control indicator to permit the second application to write to the protected value.

7. (Previously Presented) The method of Claim 4, wherein restoring the access control indicator to prohibit further modification by the second application includes returning ownership of the registry key that the ACL secures to the operating system.

8. (Previously Presented) The method of Claim 1, further comprising:

displaying, in association with the approval user interface, the prioritized user choice setting along with options for modifying the prioritized user choice setting,

wherein receiving input from the user approving the modification of the prioritized user choice setting comprises receiving input from the user in accordance with at least one of the displayed options.

9. (Previously Presented) The method of Claim 1, further comprising generating a change notification when the prioritized user choice setting has been modified, the change notification identifying the second application and the prioritized user choice setting before and after the modification.

10. (Previously Presented) The method of Claim 1, wherein the prioritized user choice setting includes at least one of a user preference relating to a file association, an autoplay setting, contents of a start menu, a registered client setting, a protocol handler, a MIME type handler, a task association, a Web browser home page, a reset Web page setting, and a sidebar setting.

11. (Previously Presented) The method of Claim 10, wherein the prioritized user choice setting includes the registered client setting, and wherein the registered client setting includes at least one of a Web browser, e-mail, media player, instant messaging, and virtual machine for Java setting.

12. (Previously Presented) A system for storing user choice settings in a data repository to prevent undesired modifications to user choice settings, the system comprising:

a registry for storing a user choice setting associated with a first application as a protected value in a registry key, wherein the user choice setting determines at least one property of execution of at least one event of the first application, and wherein the user choice setting comprises at least one of a user preference relating to a file association, an autoplay setting, contents of a start menu, a registered client, a protocol handler, a MIME type handler, a task association, an internet explorer home page, a reset Web page setting, and a sidebar setting;

an access control list (ACL) to secure the registry key, wherein the ACL prevents the first application or another application from modifying the user choice setting associated with the first application; and

an approval user interface to control modifications to the user choice setting, wherein the approval user interface is generated on a computing device of the user in response to receiving a request from the first application or another application to modify the user choice setting, and wherein the approval user interface, upon obtaining approval to modify the user choice setting,

modifies the ACL to permit writing to change the protected value in the registry key to a modified user choice setting.

13. (Previously Presented) The system of Claim 12:

wherein the approval user interface restores the ACL to prevent writing to the protected value in the registry key after writing the modified user choice setting,

and wherein the approval user interface notifies the user whenever the approval user interface writes to the protected value, including notifying the user of a content of the protected value before and after the approval user interface writes to the protected value and an identity of the application that requested the modification.

14. (Canceled).

15. (Previously Presented) The system of Claim 13, wherein the user choice setting comprises a registered client setting, and wherein the registered client setting includes at least one of a Web browser, e-mail, media player, instant messaging, and virtual machine for Java setting.

16. (Previously Presented) The system of Claim 12, wherein the computing device of the user includes an operating system having a security subsystem, and wherein the security subsystem modifies the ACL to permit the first application or another application to modify the user choice setting associated with the first application upon receiving user approval of the request to modify the user choice setting.

17. (Previously Presented) The system, of Claim 12, wherein the security subsystem modifies the ACL to permit writing to the protected value in the registry key by providing to the user ownership of the registry key, wherein ownership of the registry key automatically provides to the user rights to modify the ACL in accordance with the security subsystem of the operating system.

18. (Previously Presented) The system of Claim 12, wherein the security subsystem modifies the ACL to permit writing to the protected value in the registry key includes by providing to the user temporary ownership of the registry key, wherein temporary ownership of the registry key automatically provides to the user rights to temporarily modify the ACL in accordance with the security subsystem of the operating system.

19. (Previously) Computer-accessible storage media ("media") having components for performing a method of safely modifying user application preferences for when and how an application is to operate on a computer of a user, the method comprising:

recognizing user input data relevant to the application as a prioritized user choice setting, wherein the prioritized user choice setting determines at least one property of execution of at least one event of the application;

securing the prioritized user choice setting as a protected value using an access control indicator, wherein the access control indicator prohibits the application from modifying the prioritized user choice setting;

receiving a request from the application to modify the prioritized user choice setting;

in response to the request from the application to modify the prioritized user choice setting, generating an approval user interface requesting authorization from the user to modify the prioritized user choice setting in accordance with the modification request received;

receiving input from the user approving modification of the prioritized user choice setting associated with the application to be consistent with a value stated in the request received from the application;

modifying the access control indicator to permit modification of the prioritized user choice setting associated with the application to match the value stated in the request received from the application;

modifying the prioritized user choice setting to match the value stated in the request received from the application in accordance with the received user input;

restoring the access control indicator to prohibit further modification of the prioritized user choice setting; and

generating a change notification to the user once the prioritized user choice setting has been modified.

20. (Previously Presented) The media of Claim 19, wherein the computer of the user includes an operating system having a registry,

wherein the protected value is a registry key stored in the registry,

wherein the access control indicator an access control list (ACL) that has been initialized to prevent writing to the protected value,

and wherein modifying the access control indicator includes modifying the access control indicator to permit writing to the protected value.

21. (Previously Presented) The media of Claim 20, wherein the operating system also includes a security subsystem, and wherein modifying the access control indicator to permit writing to the protected value includes providing to the user rights to modify the ACL in accordance with the security subsystem of the operating system.

22. (Previously Presented) The media of Claim 21, wherein modifying the access control indicator to permit writing to the protected value includes providing to the user ownership of the registry key that the ACL secures, and wherein ownership of the registry key automatically provides to the user rights to modify the ACL in accordance with the security subsystem of the operating system.

23. (Previously Presented) The media of Claim 20, wherein providing to the user ownership of the registry key that the ACL secures includes temporarily providing to the user ownership of the registry key that the ACL secures.

24. (Previously Presented) The media of Claim 21, wherein modifying the access control indicator to permit modification of the prioritized user choice setting associated with the application to be consistent with the modification request received includes requiring user to modify the access control indicator to permit writing to the protected value in accordance with the security subsystem of the operating system.

25. (Previously Presented) The media of Claim 24, wherein restoring the access control indicator to prohibit further modification of the prioritized user choice setting includes returning ownership of the registry key that the ACL secures to the operating system.

26. (Canceled).

27. (Previously Presented) The media of Claim 19, wherein the change notification identifies the application and the contents of the prioritized user choice setting before and after the modification.

28. (Previously Presented) The media of Claim 19, wherein the user choice setting includes at least one of a user preference relating to a file association, an autoplay setting, contents of a start menu, a registered client setting, a protocol handler, a MME type handler, a task association, a Web browser home page, a reset Web page setting, and a sidebar setting.

29. (Previously Presented) The media of Claim 28, wherein the prioritized user choice setting includes the registered client setting, and wherein the registered client setting includes at least one of a Web browser, e-mail, media player, instant messaging, and virtual machine for Java setting.

IX. EVIDENCE APPENDIX

Not applicable

X. RELATED-PROCEEDINGS APPENDIX

Not applicable